طرق القضاء على اخطر انواع الفيروسات
بواسطة نظام الدوس وبعض اعدادات الوندوز

Way of clear your computer from virus by dos operating system
&
some application of windows

بواسطة المهندس علي حميد ياسر الياسري

By

Engeneering : ALI HAMED YASER AL YASRY
alih_eng@hotmail.com

في البداية أحب ان انوه الى ان كل ما هو مكتوب في هذا الكتاب من حقوق فكريه وطرق هي تنم عن تجربه شخصيه وممارسه عمليه مدعومه بالصور والشرح اقدمها الى اخواني من القراء ليستنيروا الى نورهم نورا.

زكاة العلم تعليمه

مقدمه عن الكاتب :

المهندس علي حميد ياسر الياسري
بكالوريوس هندسة الحاسبات والبرمجيات - الجامعة المستنصريه
السكن – محافظة ذي قار
اجيد العديد من لغات البرمجه (
c,c++,java,php,html,xml,asp,prolog,matlab,visual basic,vbscript,java script).

اجيد تصميم وادارة المواقع باشكال مختلفه.



أولا : التخلص من المشكله التي يتسبب بها فيروس هذا الفيروس ولحد هذا التاريخ 20-1-2009

يصيب الادمنستر لم يستطع أي نوع من انواع الإانتي فيروس باكتشافه ومعالجته
*مجهول الاسم والهويه.
ويقوم بتعطيل نافذة ال
(windows task manager)

باظهار رسالة تحذيريه

Alert

Task manager has been disabled by your administrator

ولا تتمكن من فتح هذه النافذه السحريه التي لها دور مهم بادارة العديد من المهام الخاصه

ولحل هذه المشكله قم بالتالي :

Run-gpedit.msc-group policy-local computer policy-user configuration-

administrative tmplate-system-ctrl+alt+del options

remove task manager

properties

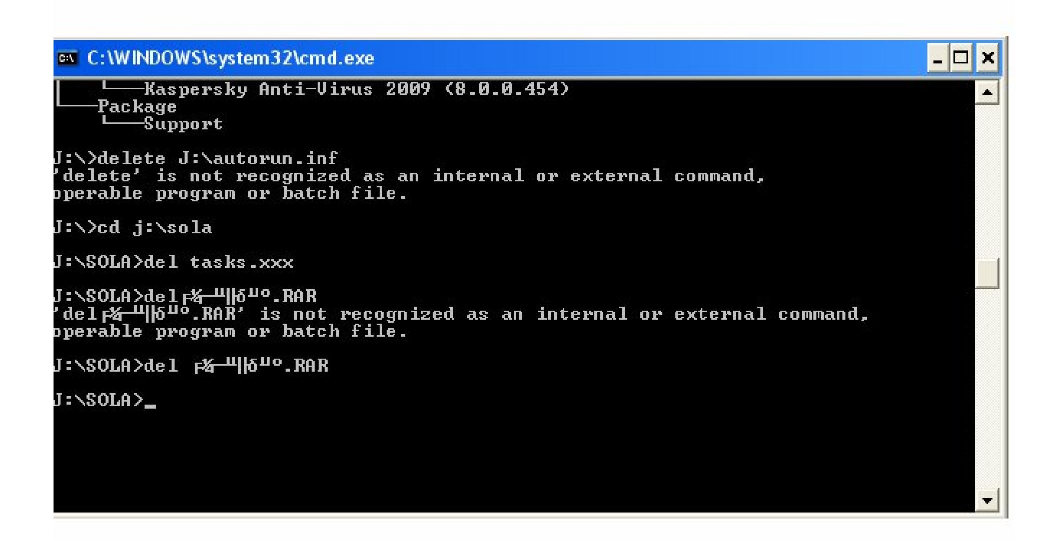
settings

disabled.

ثانيا : القضاء على عائلة فيروس

Sola
tasks.xxx
autorun.inf
sola.°لا ن ║ـلــــش ╒\RAR

والتي تحتضن العديد من الفيروسات الخطرة والتي هي مخفيه بالحقيقه وتعمل لنفسها ملفات رجوع
Backup files
وللتخلص منها توجه الى نظام الدوس واستخدم أوامر الدوس لعرض الملفات وحيث تجد الامتداد الفيروسي
ادخل به و امسح الفيروسات مسح نهائي ومن غير رجعه كما في الامثله المصوره التاليه:



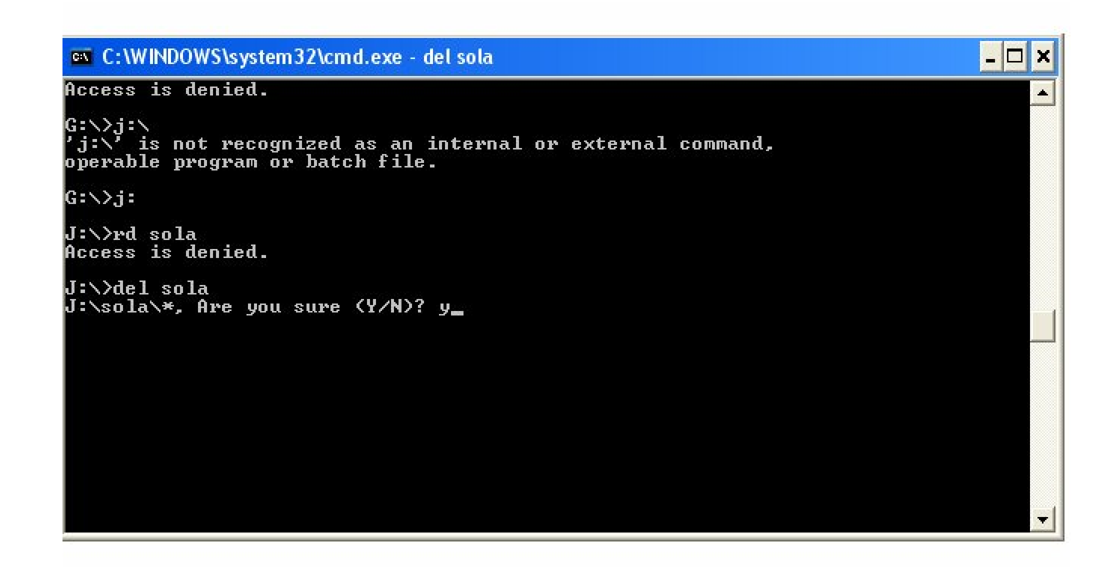

```
C:\WINDOWS\system32\cmd.exe
 ├──Avira AntiVir Premium Security Suite 2008 - v8.1.0.245
 │  └──Keys
 ├──BitDefender 2009Total Security 12.0.10 32BIT
 │  └──Patch 'till 2047
 ├──ESET NOD32 Antivirus 3.0.672 Business
 ├──ESET Smart Security 3.0.672
 └──Kaspersky Anti-Virus 2009 (8.0.0.454)
Package
 └──Support

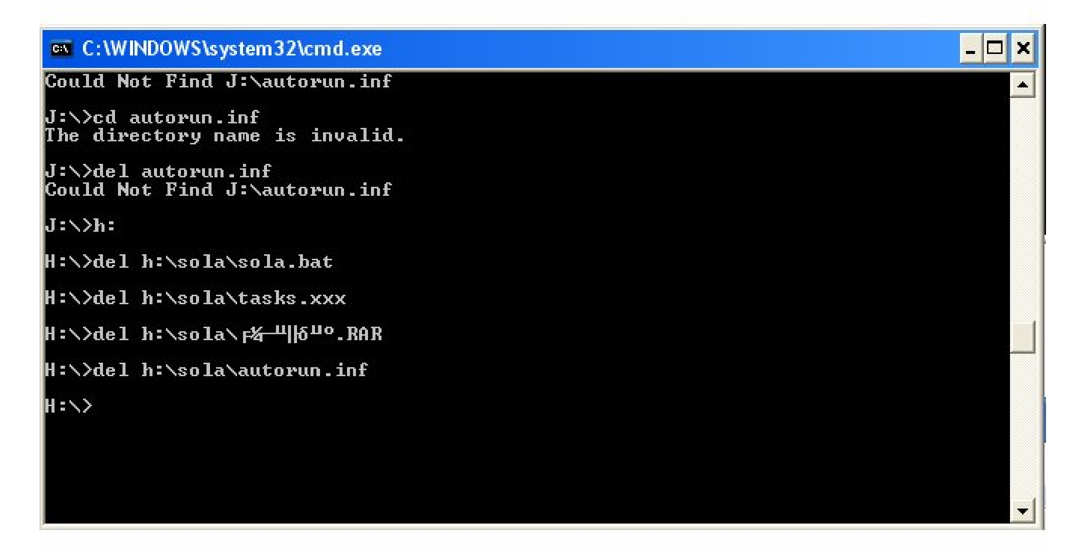
J:\>delete J:\autorun.inf
'delete' is not recognized as an internal or external command,
operable program or batch file.

J:\>cd j:\sola

J:\SOLA>del tasks.xxx

J:\SOLA>
```


C:\WINDOWS\system32\cmd.exe - del sola
Access is denied.
G:\>j:\
'j:\' is not recognized as an internal or external command,
operable program or batch file.
G:\>j:
J:\>rd sola
Access is denied.
J:\>del sola
J:\sola*, Are you sure (Y/N)? y


C:\WINDOWS\system32\cmd.exe
Could Not Find J:\autorun.inf
J:\>cd autorun.inf
The directory name is invalid.
J:\>del autorun.inf
Could Not Find J:\autorun.inf
J:\>h:
H:\>del h:\sola\sola.bat
H:\>del h:\sola\tasks.xxx
H:\>del h:\sola\autorun.inf
H:\>

وهنا اليكم الأوامر والطرق لملاحقة وحذف الفيروسات :

Microsoft Windows XP [Version 5.1.2600[
)C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\eng>j:

J:\>dir
Volume in drive J isعلي
Volume Serial Number is B0AE-B851

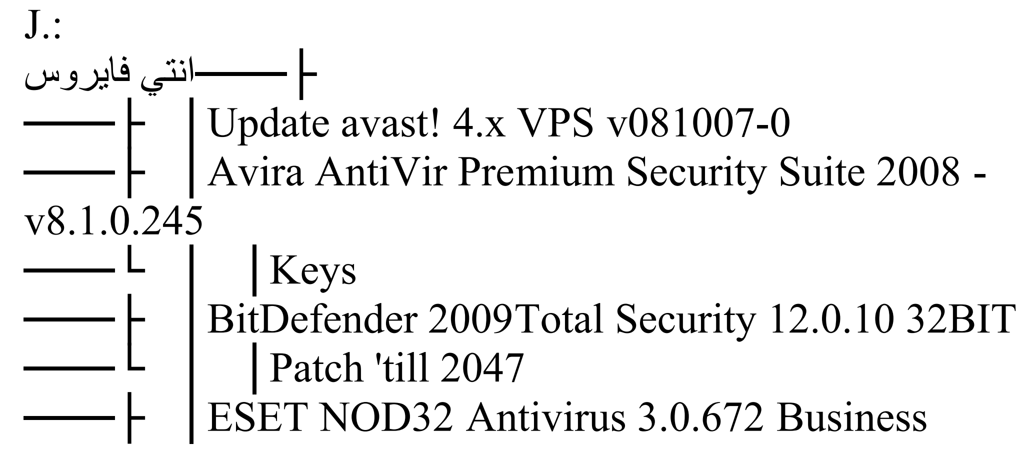
Directory of J\:

03:36 2009/21/01PM <DIRانتي فايروس <
05:00 2009/21/01PM <DIR> Package
0 File(s) 0 bytes
2 Dir(s) 69,396,480 bytes free

J:\>rd?
The filename, directory name, or volume label syntax is incorrect.

J:\>rd help
The system cannot find the file specified.

J:\>tree
Folder PATH listing for volumeعلي
Volume serial number is 0000E86E B0AE:B851
J.:



انتي فايروس───├
───├ │Update avast! 4.x VPS v081007-0
───├ │Avira AntiVir Premium Security Suite 2008 - v8.1.0.245
───└ │ │Keys
───├ │BitDefender 2009Total Security 12.0.10 32BIT
───└ │Patch 'till 2047
───├ │ESET NOD32 Antivirus 3.0.672 Business

──┝ │ESET Smart Security 3.0.672
──└ │Kaspersky Anti-Virus 2009 (8.0.0.454(
──└Package
──└ Support

J:\>delete J:\autorun.inf
'delete' is not recognized as an internal or external command,
operable program or batch file.

J:\>cd j:\sola

J:\SOLA>del tasks.xxx

J:\SOLA>del.°╨ ن║╨──ش ╒RAR
'del.°╨ ن║╨──ش ╒RAR' is not recognized as an internal or
external command,
operable program or batch file.

J:\SOLA>del.°╨ ن║╨──ش ╒ RAR

J:\SOLA>cd..

J:\>rd j:\sola
Access is denied.

J:\>rd sola
Access is denied.

J:\>g:

G:\>rd j:\sola
Access is denied.

G:\>rd j:\sola
Access is denied.

G:\>j\:

```
'j:\' is not recognized as an internal or external command,
operable program or batch file.

G:\>j:

J:\>rd sola
Access is denied.

J:\>del sola
J:\sola\*, Are you sure (Y/N)? y

J:\>del J:\autorun.inf
Could Not Find J:\autorun.inf

J:\>cd autorun.inf
The directory name is invalid.

J:\>del autorun.inf
Could Not Find J:\autorun.inf

J:\>h:

H:\>del h:\sola\sola.bat

H:\>del h:\sola\tasks.xxx

H:\>del h:\sola.°ﻻ ن║╨──ش ╒\RAR

H:\>del h:\sola\autorun.inf

H:\>del H:\SOLA
Could Not Find H:\SOLA*\

H:\>del sola
Could Not Find H:\sola*\

H:\>del sola
```

```
Could Not Find H:\sola*\

H:\>rd  sola
Access is denied.

H:\>del sola
Could Not Find H:\sola*\

H:\>del sola
Could Not Find H:\sola*\

H:\>del sola
Could Not Find H:\sola*\

H:\>del sola
Could Not Find H:\sola*\

H:\>del sola
Could Not Find H:\sola*\

H:\>del sola
Could Not Find H:\sola*\

H:\>del sola
Could Not Find H:\sola*\

H:\>g:

G:\>del j:\sola
j:\sola\*, Are you sure (Y/N)? y

G:\>del h:\sola
Could Not Find h:\sola*\

G:\>del sola
G:\sola\*, Are you sure (Y/N)? y
```

```
G:\>c:

C:\Documents and Settings\eng>cd\

C:\>del sola
C:\sola\*, Are you sure (Y/N)? y

C:\>d:

D:\>del sola
D:\sola\*, Are you sure (Y/N)? y

D:\>e:

E:\>del sola
E:\sola\*, Are you sure (Y/N)? y

E:\>f:

F:\>del sola
F:\sola\*, Are you sure (Y/N)? y

F:\>i:
The device is not ready.

F:\>g:

G:\>del sola
G:\sola\*, Are you sure (Y/N)? y

G:\>del tasks.xxx
Could Not Find G:\tasks.xxx

G:\>del sola
G:\sola\*, Are you sure (Y/N)? y
```

